ᦁ

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,426	07/09/2004	Chenming Chuang	22171-00018-US1	4425

30678   7590   04/02/2007

CONNOLLY BOVE LODGE & HUTZ LLP
P.O. BOX 2207
WILMINGTON, DE 19899-2207

EXAMINER
AVERY, JEREMIAH L

ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _09 July 2004_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-14_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-14_ is/are rejected.

7)☒ Claim(s) _3 and 7_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _09 July 2004_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-14 have been examined.

Claim Objections

1.   Claim 3 is objected to because of the following informalities: lack of clarification. The limitation, "responding to the key confirmation message with a downloading message to allow the slave cryptographic unit retrieving requested information" does not specify a function of the "slave cryptographic unit" after it conducts "retrieving requested information". The Examiner will broadly interpret the claim as "to allow the slave cryptographic unit *to retrieve* requested information". Appropriate correction is required.

2.   Claim 7 is objected to because of the following informalities: missing word. In line 3, "to validate an initial held by the slave cryptographic unit", does not specify as to what is being validated. For the purposes of examination, the Examiner will broadly interpret the limitation to be pertaining to "an initial key". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3.   Claims 7 and 9 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4.   Claim 7 recites the limitation "the rest message" in line 2. There is insufficient antecedent basis for this limitation in the claim.

5.   Claim 9 recites the limitation "the resent message" in line 3. There is insufficient

antecedent basis for this limitation in the claim.

6.   For purposes of examination, the Examiner will interpret "the rest message" and

"the resent message" as the "reset message" as found in claim 1. Appropriate

correction is required.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public
use or on sale in this country, more than one year prior to the date of application for patent in the United
States.

Claims 1-14 are rejected under 35 U.S.C. 102(b) as being anticipated by United

States Patent No. 6,233,565 to Lewis et al., hereinafter Lewis.

7.   Regarding claim 1, Lewis teaches a method of secure data exchange between a

master cryptographic unit and a slave cryptographic unit, comprising the steps of:

sending either a reset message or a key validation message to request the master

cryptographic unit to validate a key held by the slave cryptographic unit (column 15,

lines 47-64, "entries are checked against the customer record in the Master Database

305", column 19, lines 60-67, column 20, lines 1-15 and 57-67, column 21, lines 64-67,

column 22, lines 1-9, 16-25 and 42-67, column 23, lines 1-22 and 35-48, "session keys

exchanged", column 24, lines 16-37 and 54-67, column 25, lines 1-28 and 53-67,

column 26, lines 1-12, column 28, lines 14-28 and 50-67, column 29, lines 1-35 and 49-

67, column 30, lines 1-9, 14-29, column 31, lines 5-15 and column 32, lines 34-39);

forwarding a key exchange message, which includes a new key encrypted through the

key held by the slave cryptographic unit, from the master cryptographic unit to the slave

cryptographic unit (column 15, lines 47-64, "the customer 2n will receive a public key

and a private key pair file in encrypted form from the web server 150", column 19, lines 60-67, column 20, lines 1-15 and 57-67, column 21, lines 64-67, column 22, lines 1-9, 16-25 and 42-67, column 23, lines 1-22 and 35-48, "session keys exchanged", column 24, lines 16-37 and 54-67, column 25, lines 1-28 and 53-67, column 26, lines 1-12, column 28, lines 14-28 and 50-67, column 29, lines 1-35 and 49-67, column 30, lines 1-9, 14-29, column 31, lines 5-15 and column 32, lines 34-39).

8.   Regarding claim 2, Lewis teaches a step of sending a key confirmation message to notify the master cryptographic unit that the new key is correctly received by the slave cryptographic unit (column 25, lines 1-28 and 61-67, column 26, lines 1-12, column 28, lines 20-28 and 50-67, column 29, lines 1-40, "recipient uses the hash to ensure message integrity" and lines 49-67, "mailed to the client", column 30, lines 1-29 and column 32, lines 34-39).

9.   Regarding claim 3, Lewis teaches responding to the key confirmation message with a downloading message to allow the slave cryptographic unit retrieving requested information (column 11, lines 46-57, "customer then downloads the client software program for operating the system", column 15, lines 47-67, "If the customer number and password are valid, the download will proceed", column 16, lines 1-4 and column 22, lines 50-57);

sending a finish message to the master cryptographic unit after the requested information is completely downloaded (column 16, lines 18-43, column 17, lines 4-15, "A 'result' code is passed back to the purchase server 190 to indicate whether the credit card has been approved or not" and column 29, lines 20-26, "the protocol is complete").

10.   Regarding claim 4, Lewis teaches wherein the reset message requests the master cryptographic unit to validate an initial key held by the slave cryptographic unit (column 4, lines 18-35, column 6, lines 1-15, column 15, lines 47-64, column 18, lines 2-8, "confirming the success or failure of the transaction", column 19, lines 60-67, column 20, lines 61-67, column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4", column 24, lines 16-33, column 28, lines 50-61, column 29, lines 20-35 and column 32, lines 34-39).

11.   Regarding claim 5, Lewis teaches wherein the initial key is either pre-configured by factories and permanently stored in the slave cryptographic unit or obtained from the master cryptographic unit through a manual login (column 11, lines 46-66, column 15, lines 47-64, "the customer 2n will receive a public key and a private key pair file in encrypted form from the web server 150", column 22, lines 2-9 and 42-67, column 23, lines 1-8, column 24, lines 16-33, column 28, lines 21-28 and 50-67, column 29, lines 1-11 and 49-62, "server 4 initially produces the client authentication keys" and column 30, lines 13-29).

12.   Regarding claim 6, Lewis teaches a step of notifying the slave cryptographic unit that the key is invalid after the key validation message is sent (column 20, lines 61-67, "Invalid information will be identified once valid information is provided", column 29, lines 62-67 and column 30, lines 1-11, "After a client 2n authenticates with the server 4, the server 4 will notify the client if the keys have expired").

13.   Regarding claim 7, Lewis teaches a step of sending the rest message to request the master cryptographic unit to validate an initial held by the slave cryptographic unit

(column 4, lines 18-35, column 6, lines 1-15, column 15, lines 47-64, column 18, lines 2-8, "confirming the success or failure of the transaction", column 19, lines 60-67, column 20, lines 61-67, column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4", column 24, lines 16-33, column 28, lines 50-61, column 29, lines 20-35 and column 32, lines 34-39).

14.   Regarding claim 8, Lewis teaches sending another key validation message to request the master cryptographic unit to validate the new key held by the slave cryptographic unit (column 4, lines 18-35, column 6, lines 1-15, column 15, lines 47-64, column 18, lines 2-8, "confirming the success or failure of the transaction", column 19, lines 60-67, column 20, lines 61-67, column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4", column 23, lines 10-22, "re-generate a new pair of public and private keys 532", column 24, lines 16-33, column 28, lines 50-61, column 29, lines 20-35 and column 32, lines 34-39);

forwarding another key exchange message, which includes a renewed key encrypted through the new key held by the slave cryptographic unit (column 4, lines 18-35, column 6, lines 1-15, column 15, lines 47-64, column 18, lines 2-8, "confirming the success or failure of the transaction", column 19, lines 60-67, column 20, lines 61-67, column 22, lines 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a client 2n to the server 4", column 23, lines 10-22, "re-generate a new pair of public and private keys 532" and lines 36-48, column 24, lines 16-33, column 28, lines 50-61, column 29, lines 20-35 and column 32, lines 34-39).

15.   Regarding claim 9, Lewis teaches a step of notifying the slave cryptographic unit that the key is invalid after the resent message is sent (column 20, lines 61-67, "Invalid information will be identified once valid information is provided", column 29, lines 62-67 and column 30, lines 1-11, "After a client 2n authenticates with the server 4, the server 4 will notify the client if the keys have expired").

16.   Regarding claim 10, Lewis teaches wherein the master cryptographic unit is a key distribution server (column 15, lines 47-64, "the customer 2n will receive a public key and a private key pair file in encrypted form from the web server 150", column 19, lines 60-67, column 20, lines 1-15 and 57-67, column 21, lines 64-67, column 22, lines 1-9, 16-25 and 42-67, column 23, lines 1-22 and 35-48, "session keys exchanged", column 24, lines 16-37 and 54-67, column 25, lines 1-28 and 53-67, column 26, lines 1-12, column 28, lines 14-28 and 50-67, column 29, lines 1-35 and 49-67, column 30, lines 1-9, 14-29, column 31, lines 5-15 and column 32, lines 34-39).

17.   Regarding claim 11, Lewis teaches wherein the key distribution server is included in an automatic provisioning system (column 15, lines 47-64, "If the customer number and password are valid, the download will proceed", column 23, lines 35-48, column 24, lines 16-33 and column 35, lines 51-62).

18.   Regarding claim 12, Lewis wherein the slave cryptographic unit is a client (column 15, lines 47-64, "the customer 2n will receive a public key and a private key pair file in encrypted form from the web server 150", column 19, lines 60-67, column 20, lines 1-15 and 57-67, column 21, lines 64-67, column 22, lines 1-9, 16-25 and 42-67, "Key File will contain the necessary information to uniquely identify and authenticate a

client 2n to the server 4", column 23, lines 1-22 and 35-48, "session keys exchanged",

column 24, lines 16-37 and 54-67, column 25, lines 1-28 and 53-67, column 26, lines 1-

12, column 28, lines 14-28 and 50-67, column 29, lines 1-35 and 49-67, column 30,

lines 1-9, 14-29, column 31, lines 5-15 and column 32, lines 34-39).

19.   Regarding claim 13, Lewis teaches wherein the reset message includes an initial

key, a physical address of the slave cryptographic unit, timestamp data and hash data

(column 5, lines 11-26 and 54-58, column 6, lines 1-15, column 15, lines 47-64, column

19, lines 52-67, column 21, lines 39-67, "proof of valid physical address will be initially

established", column 22, lines 42-67, "Key File will contain the necessary information to

uniquely identify and authenticate a client 2n to the server 4", column 23, lines 1-22,

column 25, lines 1-15, "date/time stamp", column 27, lines 25-39, "a new user 2n would

contact the server 4 with information that uniquely identifies him/herself", column 29,

lines 1-11 and 49-67 and column 30, lines 1-11).

20.   Regarding claim 14, Lewis teaches wherein the key validation message includes

the key, a physical address of the slave cryptographic unit, timestamp data and hash

data (column 5, lines 11-26 and 54-58, column 6, lines 1-15, column 15, lines 47-64,

column 19, lines 52-67, column 21, lines 39-67, "proof of valid physical address will be

initially established", column 22, lines 42-67, "Key File will contain the necessary

information to uniquely identify and authenticate a client 2n to the server 4", column 23,

lines 1-22, column 25, lines 1-15, "date/time stamp", column 27, lines 25-39, "a new

user 2n would contact the server 4 with information that uniquely identifies him/herself",

column 29, lines 1-11 and 49-67 and column 30, lines 1-11).

21.   With regards to claims 13 and 14, it is known in the art that within a client/server environment, the location or "address" of each respective device will exist and be known between said client and server.

Conclusion

22.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following United States Patents are cited to further show the state of the art with respect to secure exchange of data within a network environment, such as:

United States Patent No. 6,757,710 to Reed which is cited to show an automated communications system that operates to transfer data, metadata and methods from a provider computer to a consumer computer through a communications network.

United States Patent No. 6,704,873 to Underwood which is cited to show a secure gateway interconnection in an e-commerce based environment.

23.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeremiah Avery whose telephone number is (571) 272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

24.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

25.   Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JLA

CHRISTOPHER REVAK
PRIMARY EXAMINER